PathAppend

The output buffer must be sized to hold at least MAX_PATH characters

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-02

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4685 bytes

Attack Category	• Path spoofing or confusion problem
Vulnerability Category	• Buffer Overflow • Unconditional
Software Context	• File Path Management
Location	• shlwapi.h
Description	The output buffer for the PathAppend() function must be sized to hold at least MAX_PATH characters. The PathAppend() function appends additional text to a path. The buffer used to return the path must be large enough to hold the returned value. The first parameter, pszPath, must be at least MAX_PATH characters in length to ensure that it is large enough to hold the returned string. Otherwise, a buffer overflow can occur. Note: If the routine fails, it NULL's the path and returns FALSE. The routine will actually stop (and give FALSE) at the 260 MAX_PATH character limit. Note: Some Unicode versions of Path functions can actually use paths that are up to 32,000 characters long by using a "\\?\" prefix on the path.
APIs	**Function Name** / **Comments** ATLPath::Append method / Overloaded wrapper of Path Append PathAppend / arg 0+1 stored in 0 PathAppendA / PathAppendW /
Method of Attack	Attacker can cause a buffer overflow if the path variable is not long enough to hold the variable. Since the appendage directory can be of arbitrary length the attacker can overflow the buffer.

1. http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

Exception Criteria	
Solutions	**Solution Applicability**: Whenever PathAppend is used. **Solution Description**: Ensure that path buffer is at least MAX_PATH in length. **Solution Efficacy**: Effective.
Signature Details	BOOL PathAppend(LPTSTR pszPath, LPCTSTR pszMore);

Examples of Incorrect Code	`// String for path name.`
	`TCHAR buffer_1[15] = TEXT("alpha \\beta"); // Note: buffer is too small!`
	`LPTSTR lpStr1;`
	`lpStr1 = buffer_1;`
	`// String of what is being added.`
	`TCHAR buffer_2[ ] = TEXT("gamma");`
	`LPTSTR lpStr2;`
	`lpStr2 = buffer_2;`
	`bool ret = PathAppend(lpStr1,lpStr2);`

Examples of Corrected Code	`// String for path name.`
	`TCHAR buffer_1[MAX_PATH] = TEXT(""alpha\\beta"); // Note: buffer is correctly sized`
	`LPTSTR lpStr1;`
	`lpStr1 = buffer_1;`
	`// String of what is being added.`
	`TCHAR buffer_2[ ] = TEXT("gamma");`
	`LPTSTR lpStr2;`
	`lpStr2 = buffer_2;`
	`bool ret = PathAppend(lpStr1,lpStr2);`

Source Reference	• http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/shlwapi/path/pathappend.asp[2]
Recommended Resource	
Discriminant Set	**Operating System**: • Windows **Languages**: • C • C++

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. mailto:copyright@cigital.com